

(12) UK Patent Application (19) GB (11) 2 385 965 (13) A

(43) Date of A Publication 03.09.2003

(21) Application No 0304270.2

(22) Date of Filing 25.02.2003

(30) Priority Data

(31) 0204589

(32) 27.02.2002

(33) GB

(71) Applicant(s)

Gordano Limited
(Incorporated in the United Kingdom)
PO Box 79, CLEVEDON, North Somerset,
BS21 6ZG, United Kingdom

(72) Inventor(s)

Brian Dorricott

(74) Agent and/or Address for Service

Withers & Rogers
Goldings House, 2 Hays Lane, LONDON,
SE1 2HW, United Kingdom

(51) INT CL⁷

G06F 17/60, H04L 12/58

(52) UK CL (Edition V)

G4A AUXB

(56) Documents Cited

WO 2001/016695 A1

WO 1999/010817 A1

(58) Field of Search

INT CL⁷ G06F, H04L

Other: Online databases: EPODOC, Full text patents,
JAPIO, WPI

(54) Abstract Title

Filtering e-mail messages for spam

(57) A method of filtering incoming e-mail messages for spam is provided which, on receipt of an incoming e-mail issues an e-mail challenge to the sender of the received e-mail requesting that they in turn send an e-mail confirmation confirming that they are the sender of the originally received e-mail, and in which received e-mails are then processed further according to whether or not they are occupied by a corresponding confirmation e-mail. Senders that provide the requested e-mail confirmation can be added to an approved list of senders such that subsequent e-mails received from them are not challenged again, whilst those e-mails to which an e-mail confirmation is not received in response to the issued challenge can be deleted from the user's e-mail system and the sender added to a blocked list of senders such that subsequent e-mails from a blocked sender are automatically ignored. The e-mail challenge may be sent from a unique e-mail address created in response to the receipt of the originally received e-mail.

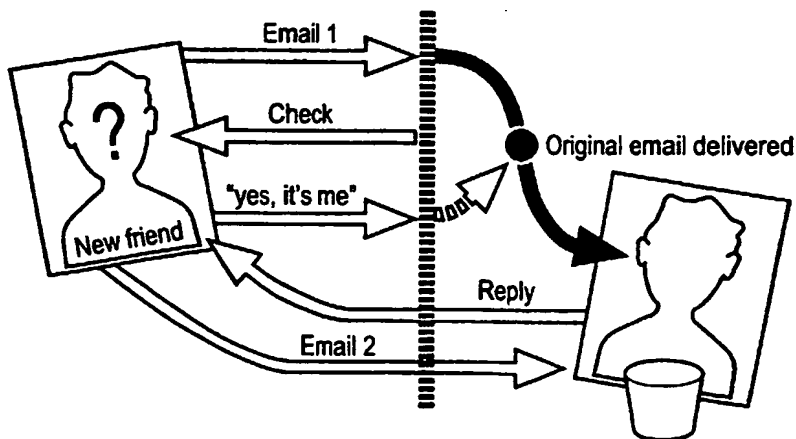


Fig. 1

1/2

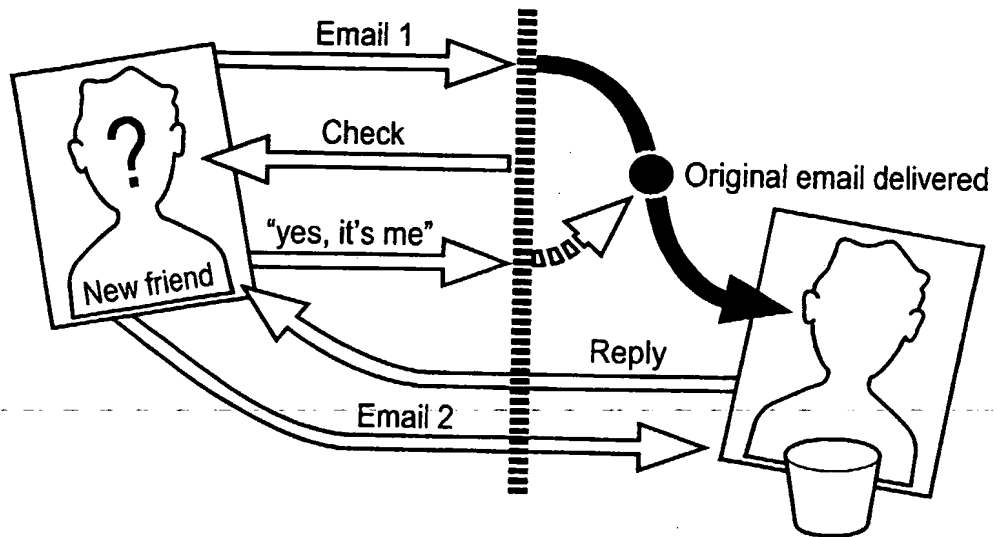


Fig. 1

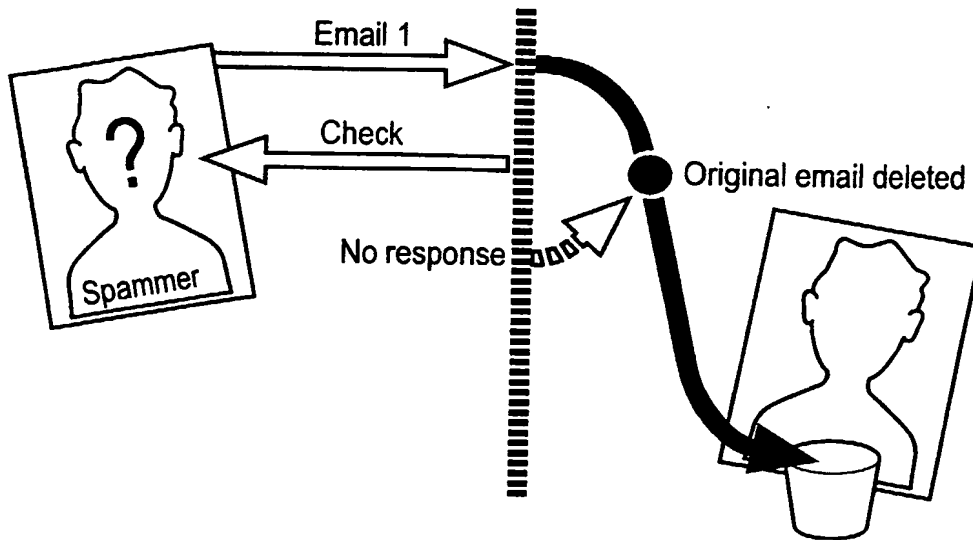


Fig. 2

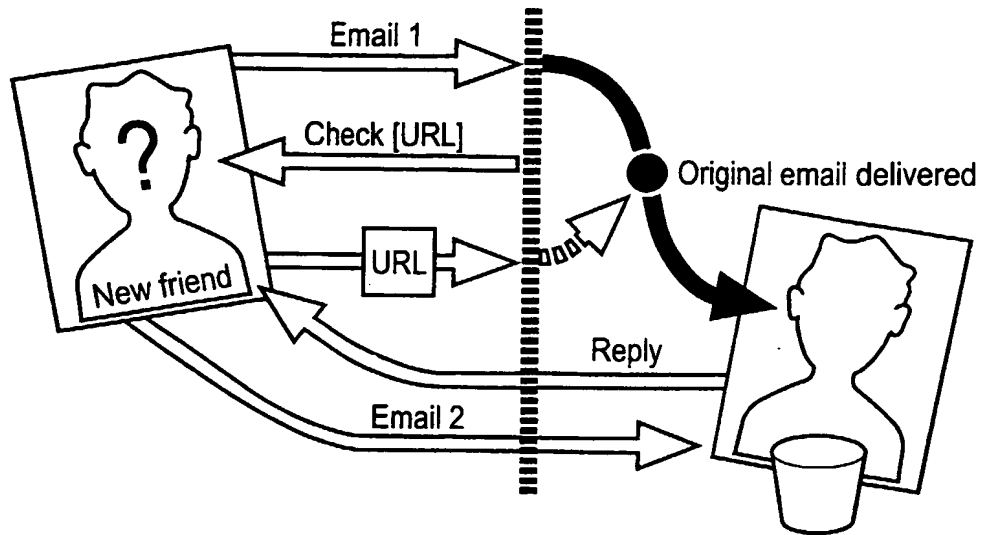


Fig. 3

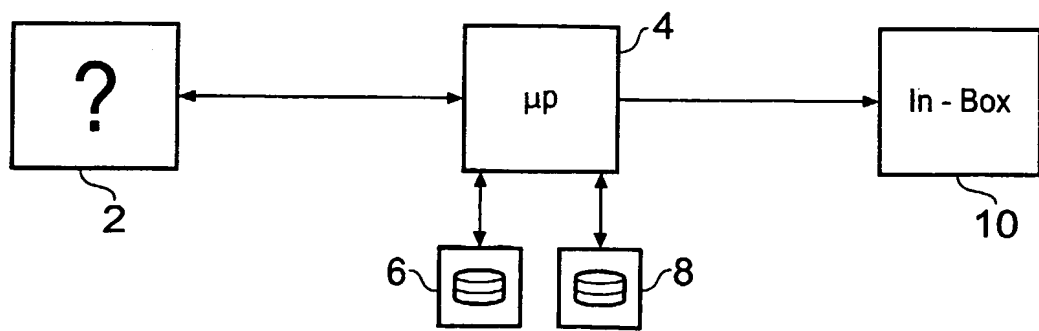


Fig. 4

FILTERING E-MAIL MESSAGES

This invention relates to the filtering of incoming e-mail messages.

Spam is the name given to unsolicited e-mail messages that are sent to people indiscriminately. These messages might also be inappropriate. For example, an e-mail message offering cheap contact lenses might be inappropriate if sent to people with unimpaired vision. A contact lens user could, however, consider the message to be of value, even though it was unsolicited. This example illustrates a major issue with such e-mail; only the recipient of a message can truly decide whether it is spam or not.

Filters are known to check e-mails for spam using several techniques. For example:

- **Filters.** The software looks for key words (e.g. XXX, sex, etc.). When a keyword is found the e-mail message is rejected.
- **Compliance checking.** A considerable number of tools used by spammers generate "non-compliant" e-mail messages. These can be identified and ignored.
- **Traffic Anomaly Detection.** Monitoring where e-mail messages come from and go to will help to detect unusual patterns of e-mail that are often associated with mass mailings. Software can be configured to take action when specific limits are reached.

All of these known filters have several problems including:

- **Maintenance.** Maintaining a word list for filters can become a full time job for the systems administrator.
- **False positives.** A false positive occurs when a normal, legitimate message is incorrectly identified as spam. Filtering on a keyword such as "breast" will catch all discussions on "breasts" including those concerning say, cancer treatment.

The present invention provides an improved filtering technique for incoming e-mails in which, on receiving an e-mail, an e-mail challenge is sent to the sender of the e-mail requesting that they send an e-mail confirmation that they are the sender of the original

e-mail, and in which received e-mails are then processed further according to whether or not they are accompanied by a corresponding confirmation e-mail. Optionally the present invention allows for a time period to be set in which the validation e-mail must be sent. If the validation is not received, the message and record of the address will be deleted. If a valid confirmation is received then the address can be flagged as a permanently acceptable address.

This filtering technique has a number of advantages as follows:

Is easy to understand.

- Is easy to use.
- Saves time. Removing the need for users to review spam increases the time available to handle legitimate e-mail.
- Reduces the number of false positives. Users no longer need to review their in-box when deleting spam. This dramatically reduces the likelihood that they delete legitimate e-mail accidentally.
- Can be used with any mail client. The confirmation process can be used irrespective of mailbox access method. If a mail server is also configured for POP3/IMAP using, say GLMail, then with any POP3 or IMAP4 mail client (e.g. Microsoft Outlook, Microsoft Outlook Express, Qualcomm's Eudora, etc.) can be used in addition to the server HTTP client.
- Has low management overhead. The system administrator does not have to make changes to the system set up for each user. Each user can choose their own individual settings.
- Accidental "leakage" of a users e-mail address is limited.
- Commonly SPAM is sent from addresses that are unable to receive e-mail, either because of an invalid reply address or by deliberately disabling the account. Such addresses will be caught with no user action required.

Confirmation is an additional stage in the mail handling process that requires the original sender of a message to take some action when first communicating. This action "verifies" that the sender exists and intended the message to be sent.

Once the sender has returned the verification, the original message is delivered as usual. The recipient can elect to have the sender's e-mail address automatically added to their address book, so the next time a message is received from them the confirmation is not activated. This means that the sender has to go through the process only once.

While messages are waiting confirmation, they are held in a "Quarantine" folder that may be accessed by the recipient at any time. Old messages are removed automatically from the Quarantine folder after a number of days defined by the user. If a message is removed from Quarantine without a confirmation having been received then the e-mail address can be blocked.

Embodiments of the present invention will now be described by way of illustrative example only with reference to the accompanying drawings in which:

Figure 1 shows e-mail communications between Martin and Joe, a new correspondent according to a first embodiment of the present invention;

Figure 2 shows e-mail communications between Martin and Sam the spammer according to an embodiment of the present invention.

Figure 3 shows e-mail communications according to a first embodiment of the present invention; and

Figure 4 shows an e-mail system according to an embodiment of the present invention.

As an example consider Martin and a new correspondent, Joe. Martin has just switched on confirmation for the first time. Having previously exchanged e-mail addresses with Joe at a recent conference, Joe now e-mails him for the first time (e-mail 1 Figure 1). On receipt at Martin's server, Joe's e-mail was diverted into the "Quarantine" folder. Joe is then immediately sent an automatically generated e-mail from Martin's system (check). It looks like this:

Hi!

Many thanks for your e-mail. Please reply to this message.

Martin

To explain: I have set up an anti-spam filter which asks for a confirmation from you that you intended to e-mail me. When you reply, the message will be delivered to me as usual and I can read it. You will only have to do this once.

In order for your message to be delivered to martin@dance.org.uk, please reply to this message, leaving the following lines intact.

---start

token:3c89cb835b4a941836b94bd6841f60d5:IoZ7J)Sd

---end

On receipt, Joe simply replies to the message ("yes, it's me") and does not have to type anything into the body of the message.

The reply arrives at Martin's account where the confirmation process identifies the "token" and automatically transfers Joe's e-mail into Martin's "In-Box". Martin can now reply to Joe in the usual way (reply, e-mail2, etc.). The token may be in the body, subject or in part of the return address.

In an alternative embodiment, illustrated in Figure 3, the e-mail challenge sent by Martin requests that the recipient, in this case Joe, responds by selecting a unique URL (website) to confirm that they are the sender of the originally received e-mail. By selecting the URL the 'token' embedded in the e-mail challenge is automatically passed, together with Joe's e-mail details, to the URL host and from there to Martin's server. This is accomplished by conventional means, such as Java applets.

In a further embodiment the e-mail challenge is sent from a unique e-mail address to which a response must be sent to avoid rejection of the original message. Each message that is received by Martin's e-mail server from a previously unknown source causes a new e-mail account to be generated from which the challenge e-mail is sent. Optionally, the unique e-mail address's may be arranged to expire after a certain period of time. In either case it is not necessary, although it is not precluded either, to include an identifying token in the e-mail challenge as any reply to the unique e-mail address must have been sent from the original sender, i.e. Joe, as only they have been provided with the unique e-mail address.

There are several choices that Martin has about the way he can use the confirmation process:

- *Checking quarantined e-mail.* At any time, Martin can check the "special" folder called "Quarantine". This folder contains all the messages waiting for the confirmation response from the sender. After a chosen number of days, messages are removed from the folder automatically. When messages are removed, the sender's e-mail address can be added to the "block list" so messages from this person are never accepted again. Martin can choose to block, accept or delete any messages at any time at his discretion.
- *Changing the confirmation message.* Martin can edit the confirmation message so he can provide a personal response in his own language and style.
- *Only confirming addresses once.* Confirmation messages are only sent to those people who do not have an entry in Martin's address book. Martin could add e-mail addresses to the address book manually. To ease management, Martin can decide how which addresses are added automatically. For example, every address Martin e-mails can be placed into the address book and/or the address of anyone who goes through the confirmation process. This means that the confirmation does not affect those people that Martin already communicates with. Martin can also decide to clear his address book at any time, thus forcing a reconfirmation in the future.

Consider now the example of Sam, the spammer. Sam has just put together a mail shot to 10,000,000 people (e-mail 1 in Figure 2). In the past, Martin's in-box would have received

an e-mail containing yet another "get rich quick" idea. Now, with the confirmation process switched on, he is going to be spared from the hassle.

When Martin's system receives the message from Sam, it does not find a corresponding address book entry and so sends a confirmation message to the address in the e-mail message (check). One of two things is now likely to happen, depending upon how Sam sent his spam.

Most spam is sent from accounts that do not exist. In this case, the mail system will return a message (possibly from the "postmaster") saying that the account is not available. Since the details of this message do not match Sam's original message, the confirmation process is activated again and both messages reside in the Quarantine folder. Eventually, the messages will be deleted and the spam never reaches Martin's in-box.

If Sam sent the message from his own account he will need to personally reply to the message in order for it to be delivered to Martin. For a large number of responses, this is clearly not worth the spammer's time.

The confirmation process can be used with Microsoft Outlook, Eudora, Pegasus, etc. The Confirmation process works on the server by holding messages in a special "Quarantine" folder and then transferring it to the standard "In-Box" once a confirmation has been received. If the mail server is equipped with a suitable complement, such as GLMail or NTMail, then any mail client that can use POP3 or IMAP4 can subsequently obtain the message in the usual way. Further, those people using an IMAP4 client can also review messages that appear in the Quarantine folder. Each user need only log on GLWebMail XT once to set up their confirmation options and retains the option to access their mailbox via the inbuilt GLWebMailXT client at any time.

False positives are only likely to occur if the original sender (in this case Joe) never replies to the confirmation message and even then, only if it is the first ever communication. In this case, Martin is likely to know about the e-mail message through other means (e.g. because they met at the conference) and can simply check the Quarantine folder.

Experience has shown that confirmation actually reduces the number of false positives. When users receive a large number of spam messages (e.g. five or ten each day), they tend to simply press the "delete" button to delete anything that looks like spam. This may lead to legitimate messages being deleted carelessly or accidentally.

For example, Martin might have sent a payment for some new software. The company sends the key via e-mail with a subject title of "Amazing Slow Downer for Windows" from an addressee of "Bernadette". Since Martin doesn't recognise the name, he simply deletes the e-mail. A couple of weeks later, he rings up to find out what happened to his software!

Figure 4 illustrates schematically an e-mail system according to embodiments of the present invention. The new friend or potential spammer 2 is shown in communication with a data processor 4 that is resident in the e-mail system. The data processor 4 is in communication with two data storage areas. The first data storage area 6 stores a list of approved senders, whilst the second data storage area 8 stores a list of blocked senders. The data processor 4 is arranged to access the first and second data storage areas in response to receiving an e-mail from the sender 2 as part of the process, as described hereinbefore, of determining how to process the received e-mail. Cleared e-mails are displayed in a conventional manner in a system in Box 10.

CLAIMS

1. A method of filtering incoming e-mails, the method comprising:

on receipt of an e-mail from a sender, sending an e-mail challenge to the sender requesting that they provide confirmation that they are the sender of the originally received e-mail; and

the automatic processing of said received e-mails in accordance to whether or not the confirmation is received.

2. A method according to claim 1, wherein if said confirmation is received, said originally received e-mail is forwarded to a specified recipient.
3. A method according to any preceding claim further comprising comparing the sender to a list of one or more approved senders and if the sender is an approved sender directly processing said e-mail without sending an e-mail challenge.
4. A method according to claim 3, wherein on receipt of said confirmation, the sender of said confirmation is added to the list of approved senders.
5. A method according to any preceding claim, wherein the originally received e-mail is stored in an allocated storage location whilst receipt of the confirmation is awaited.
6. A method according to claim 5, wherein said e-mails in said storage location are removed a predetermined period of time after their receipt.
7. A method according to claim 6, wherein the senders of e-mails removed from said storage location on expiry of the predetermined time period are added to a blocked senders list.

8. A method according to claim 7, wherein e-mails from senders on the blocked senders list are not accepted.
9. A method according to any preceding claim, wherein said confirmation comprises an e-mail reply to said e-mail challenge.
10. A method according to claim 9, wherein the e-mail challenge comprises an identifying token.
11. A method according to claim 10, wherein said e-mail confirmation is accepted only if it comprises the identifying token.
12. A method according to any one of claims 9 to 11, wherein said e-mail challenge is sent from a unique e-mail address created in response to the receipt of the originally received e-mail.
13. A method according to claim 12, wherein said e-mail confirmation is accepted only if it is sent to said unique e-mail address.
14. A method according to claim 12 or 13, wherein said unique e-mail address expires a predetermined time period after being created.
15. A method according to any one of claims 1 to 8, wherein said e-mail challenge comprises an invitation to select a unique network address and said confirmation is provided by the sender of the original e-mail selecting said unique network address.
16. A method according to claim 15, wherein said e-mail challenge includes an identifying token that is arranged to be transmitted to the unique network address when it is selected.

17. A method according to claim 16, wherein the confirmation is only accepted if the identifying token is provided.
18. A computer program product comprising a plurality of program code instructions, which when run on a computer cause the computer to execute the method of any one of claims 1 to 17.
19. An e-mail system for filtering incoming e-mails, the e-mail system comprising a data processor arranged to issue an e-mail challenge to the sender of an e-mail in response to receipt of the e-mail, the e-mail challenge requesting confirmation from the e-mail sender that they are the sender of the original e-mail, and arranged to further process said received e-mail in accordance with whether or not said confirmation is received.
20. An e-mail system according to claim 19, further comprising an approved sender store arranged to store a list of approved senders and wherein said data processor is arranged to compare the sender of a received e-mail with said list and, where a match is made between said sender and the list, directly process the received e-mail without issuing an e-mail challenge.
21. An e-mail system according to claim 20, wherein said data processor is further arranged to add a sender to the list of approved senders on receipt of a confirmation from said sender.
22. An e-mail system according to claim 19, 20 or 21, further comprising a stored blocked senders list and wherein said data processor is arranged to compare the sender of an e-mail with said blocked senders list and to not accept said e-mail if a match is made.
23. An e-mail system according to any one of claims 19 to 22, wherein the data processor is further arranged to generate a unique e-mail address in response to receipt of an e-mail and to send said e-mail challenge to said sender from said unique e-mail address.

24. An e-mail system according to claim 23, wherein the data processor is arranged to accept a confirmation only if it is sent to send unique e-mail address.
25. An e-mail system according to claim 23 or 24, wherein the data processor is arranged to mark said unique e-mail address as expired a predetermined time period after generating the unique e-mail address.



INVESTOR IN PEOPLE

Application No: GB 0304270.2
Claims searched: 1-25

Examiner: Graham Russell
Date of search: 11 June 2003

Patents Act 1977 : Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
X	1-11, 18-22	WO 99/10817 A1 (COBB) see abstract, page 3 lines 4-17, page 11 lines 18-21, page 12 lines 21-24, page 20 line 18 - page 21 line 11
X	1-5, 18-22	WO 01/16695 A1 (KATSIKAS) see abstract, page 2 lines 1-33

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC^v:

--

Worldwide search of patent documents classified in the following areas of the IPC⁷:

G06F, H04L

The following online and other databases have been used in the preparation of this search report:

EPODOC, Full text patents, JAPIO, WPI

THIS PAGE BLANK (USPTO)